CHAPTER 6

Sample Scenarios

Protecting an urban environment presents several challenges, where large number of elements need to be protected from crime, natural catastrophes, terrorism, and threats to critical infrastructure.

The following sections present some sample scenarios that integrate the physical security components outlined in this design guide. Based on specific requirements and the environment being monitored, many more scenarios can be imagined and adapted to protect citizens and business by providing a quick resolution of incidents.

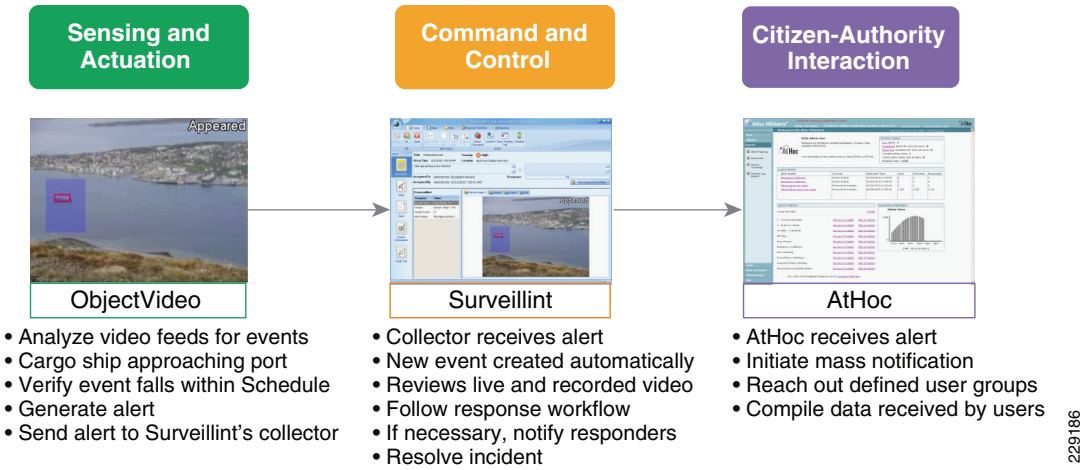
Video TripWire Crossing—Cargo Ports

Video TripWire™ crossing can have different meanings based on the location and type of sensors being used. In a large area such as an airport or oil refinery, it can mean monitoring a virtual fence line monitoring for unexpected movement. In a border situation, it can mean monitoring a state or country line or river for illegal crossings. In a train station, it can be watching for track crossings, but having the need to differentiate between a track crossing and a worker on a catwalk.

Cargo ports represent a vital part of the economy and are used to transport materials such as liquid fuels, chemicals, wood, automobiles, etc. Protecting cargo ports remains a high priority for several regions.

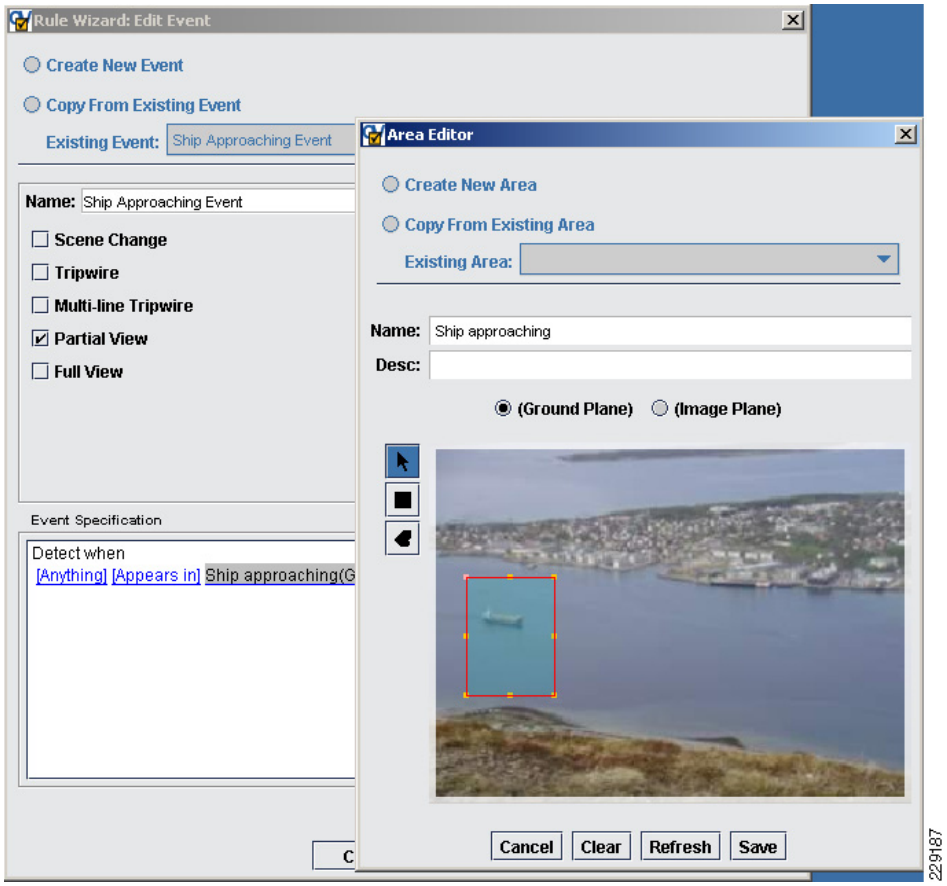
In the following example, video analytics is used to detect cargo ships approaching the port. ObjectVideo is able to detect a ship in the field of view and generates an alert to Surveillint. As shown in Figure 6-1, the alert appears in the Surveillint Operations Console and is addressed by the security operators just like any other alert. The alert may have specific workflow that the operator must follow before closing the event.

Figure 6-1 Scenario Flow



Using the ObjectVideo Rule Management Tool, define the video analytics rules to be observed by the sensor. In the example in Figure 6-2, the rule detects when a cargo ship approaches the defined area. Many other conditions can be defined to identify the ship, such as movement direction, entering or leaving the detection area, detecting time spent in the detection area, and so on.

Figure 6-2 Define Analytics Rule



When the sensor becomes active, the video analytics engine monitors for ships appearing in the field of view. The sensor and rule can also be configured using various size filters to detect only large ships and not for every possible watercraft.

The video analytics engine can be configured to monitor only during specific times, therefore reducing the number of alerts generated. The schedule in Figure 6-3 is configured to monitor for ships during evening or night time.

Figure 6-3 Detection Schedule

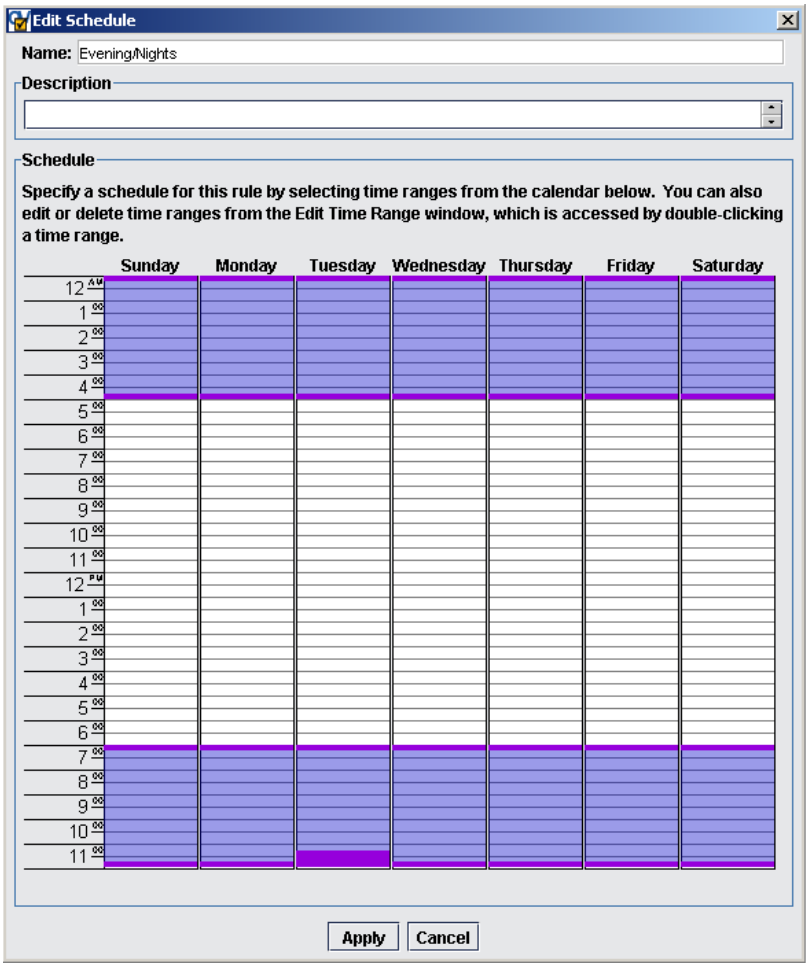
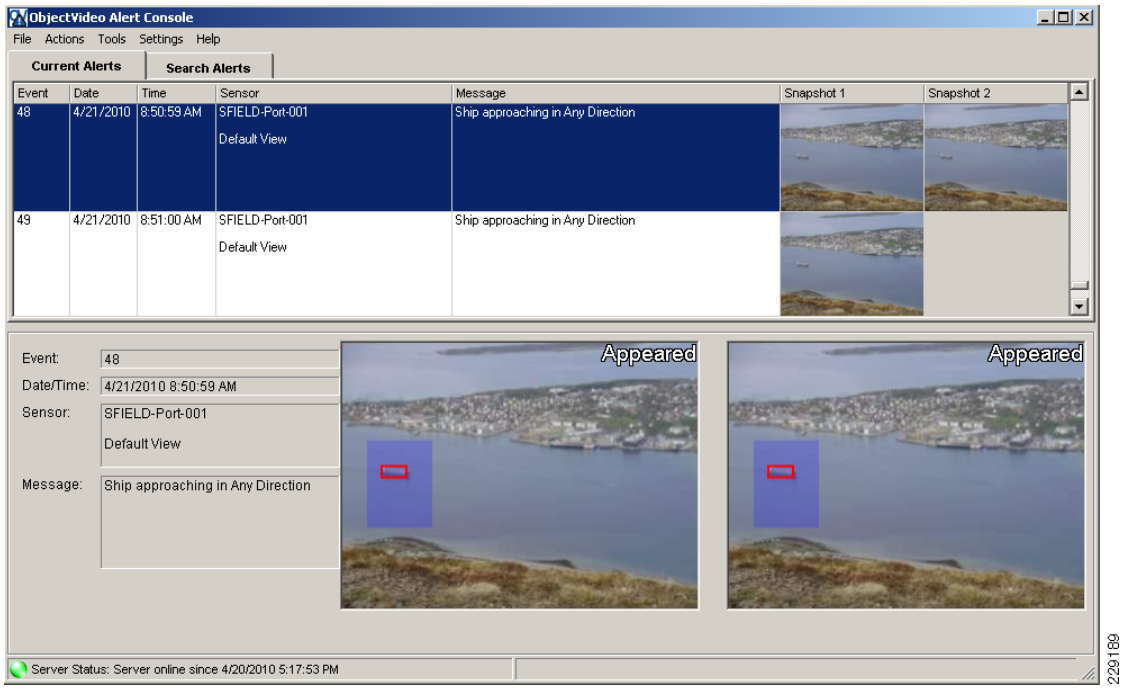


Figure 6-4 shows ObjectVideo's Alert Console detecting a ship approaching the port. The alert is logged in ObjectVideo's console and simultaneously sent to Surveillint for further analysis.

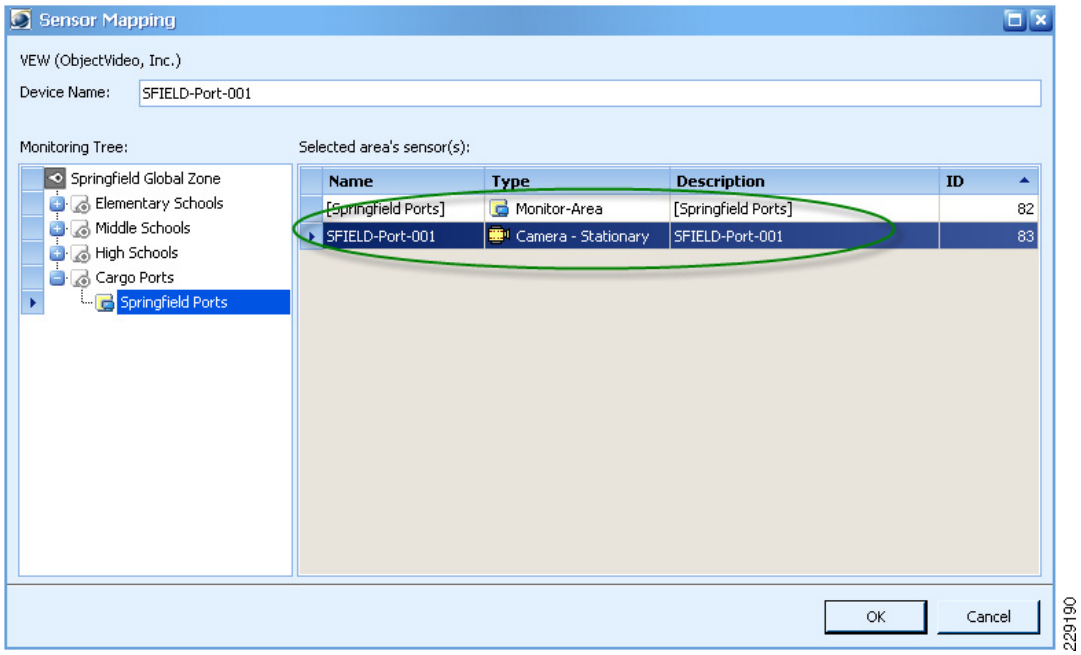
Figure 6-4 Alert Console



Before receiving alerts in Surveillint, you can define a sensor mapping between the ObjectVideo sensor and a camera sensor in Surveillint.

To do this using Surveillint's Administration Console, click on **Event Integration > Sensor Mapping** and define a mapping between SFIELD-Port-001 sensors, as shown in Figure 6-5.

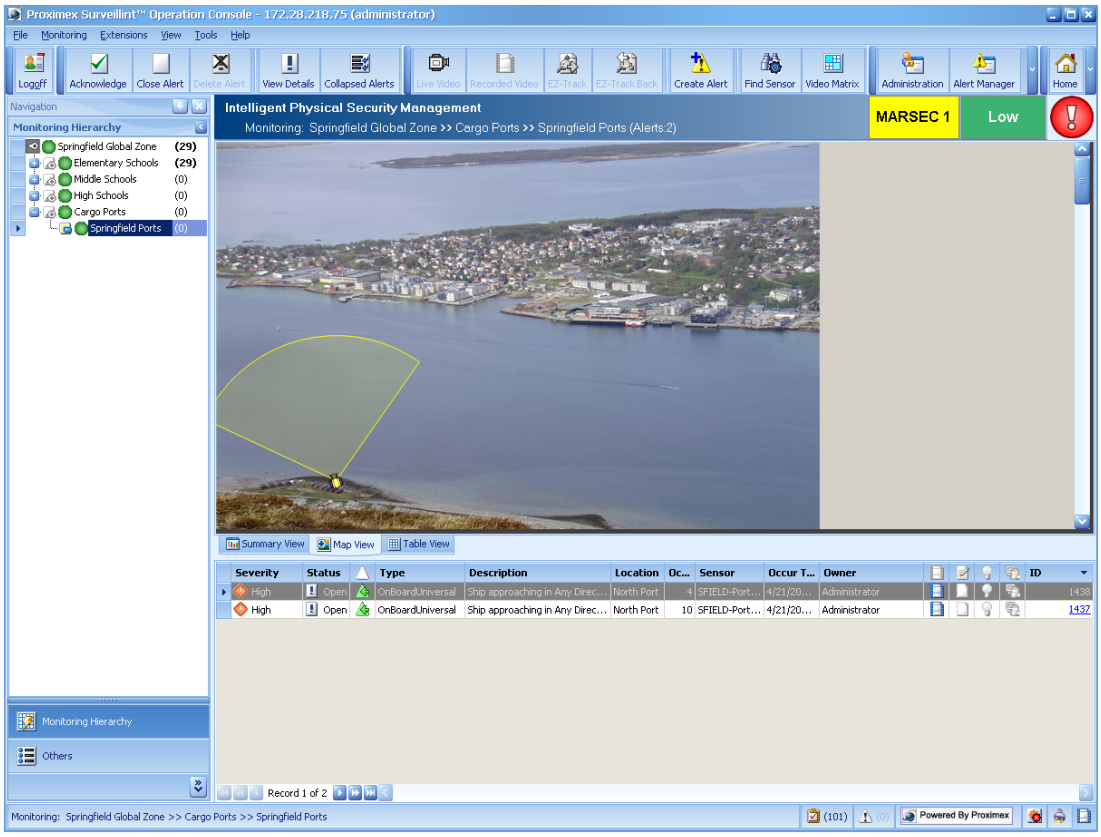
Figure 6-5 Sensor Mapping



The sensor mapping between ObjectVideo and Surveillint ensures that alerts are logged against the right sensor, making event resolution easier for the security operator.

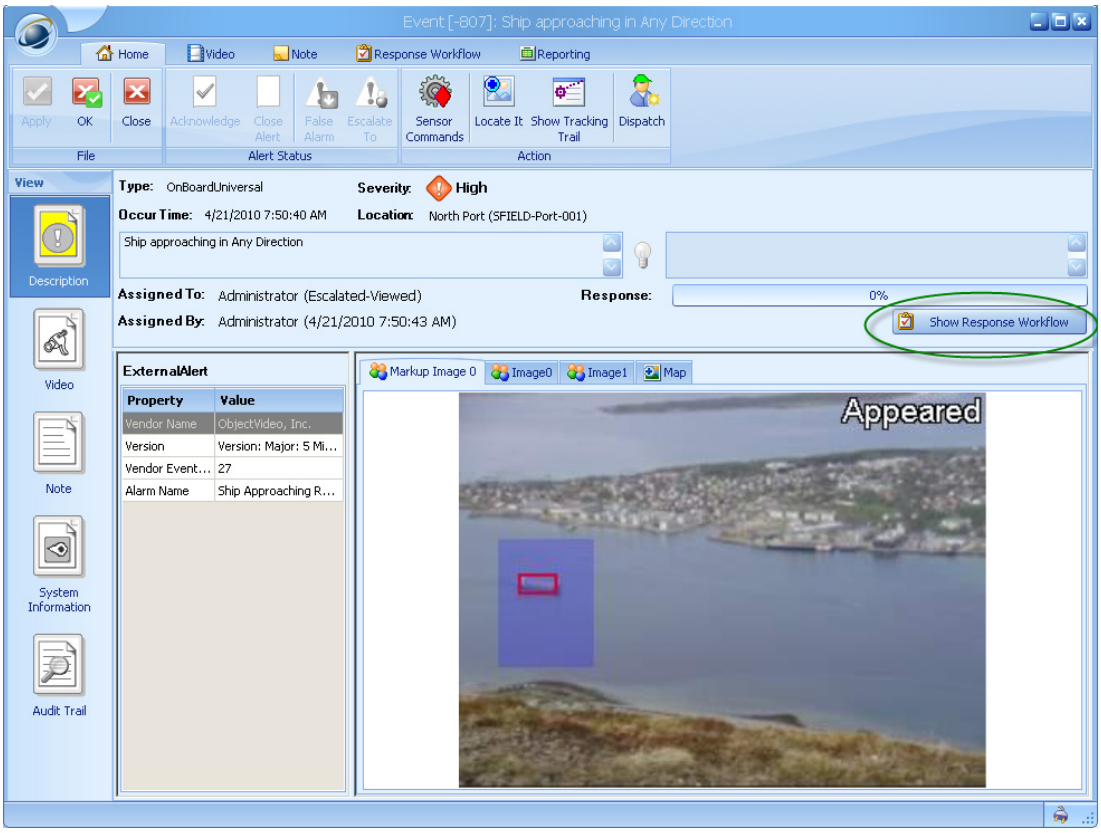
Figure 6-6 shows the monitoring area dedicated to the cargo port and the camera sensor's position in the map. The map can also be defined using actual GPS coordinates to properly identify the location of cameras and sensors.

Figure 6-6 Surveillint Monitoring Area



ObjectVideo sends the alert notification to Surveillint via the connector provided by Proximex. Surveillint logs an event in the Operation Console, as shown in Figure 6-7.

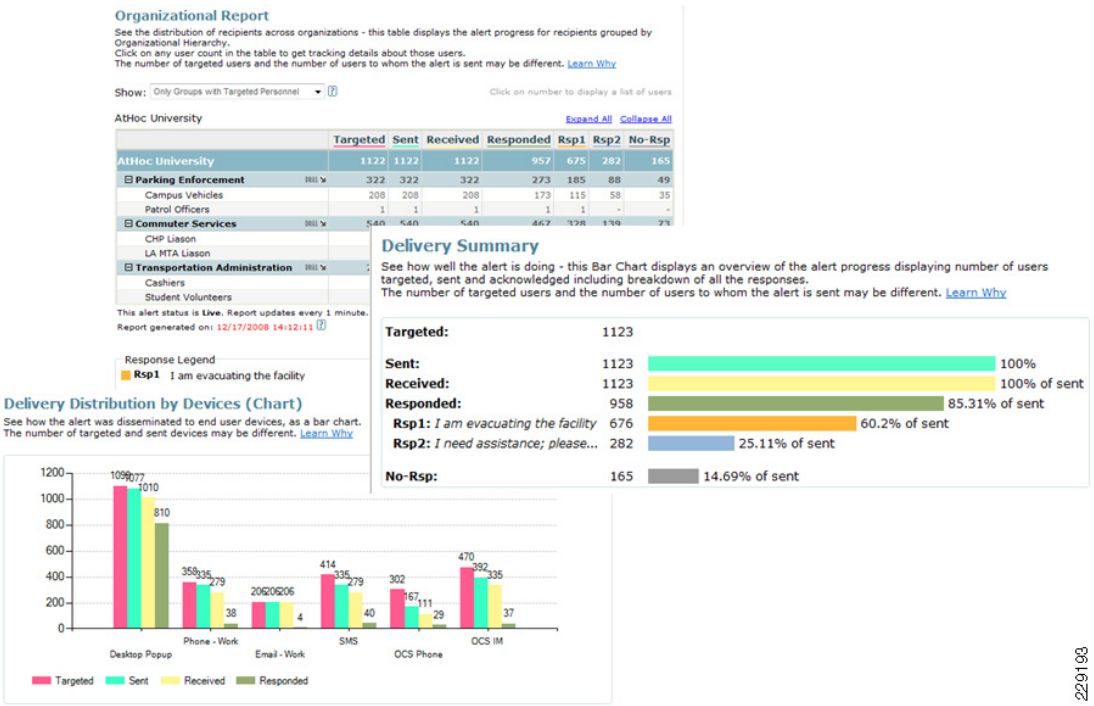
Figure 6-7 Cargo Ship Detected



The event window allows the operator to review the event and determine whether further action is required to resolve it. From the single window, the operator can perform several activities as dictated by the organizations Standard Operating Procedures (SOPs), which can be enforced in Surveillint's response workflow. Surveillint's response workflow provides step-by-step instructions for each alert that empowers the operator to perform the appropriate tasks in the appropriate order to resolve the incident. Other items that are presented to the operator include reviewing live and recorded video, dispatching emergency responders, exporting video files, escalating the alert to another operator/manager, and so on.

When an accountability alert is sent to personnel via AtHoc, all responses are tracked in real-time and compiled to show a personnel accountability graphical report (see Figure 6-8), allowing the operator to drill into the results and see who are the users that had requested help, or that had not responded.

Figure 6-8 AtHoc's Personnel Accountability Graphical Report



Unauthorized Building Access/Forced Entry

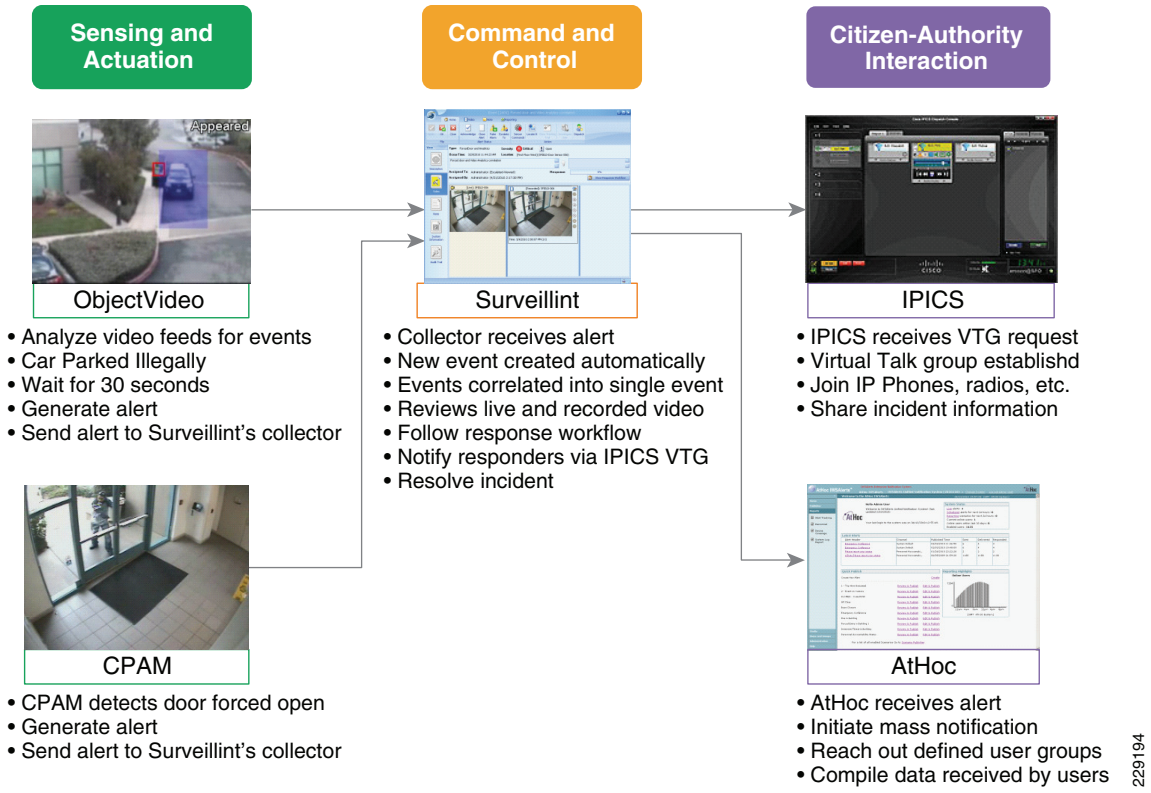
In a more complicated incident, receiving simultaneous alerts may be received from multiple systems in a short period of time. Being able to combine these alerts into a single event greatly improves the time to resolve incidents by allowing the operators to work on a single event window.

A sample scenario where two alerts get combined into a single event can be generated by both ObjectVideo and CPAM.

A car parked illegally in a restricted zone for more than 30 seconds is recognized by ObjectVideo and an alert is sent to Surveillint. By itself, the alert is generated with a low severity and can be quickly resolved by the operator after reviewing live and recorded video.

A second alert arrives from the access control system indicating that a door has been forced open. This alert was received in the general vicinity of the parking lot within a certain number of seconds. Figure 6-9 shows the scenario flow.

Figure 6-9 Scenario Flow



The alerts are combined into a single event window, with a critical severity. From a single event window, the operator is able to work on the incident. By following the response workflow, the operator may view live and recorded video, launch an IPICS Virtual Talk Group, and notify AtHoc's mass notification alerts if appropriate.

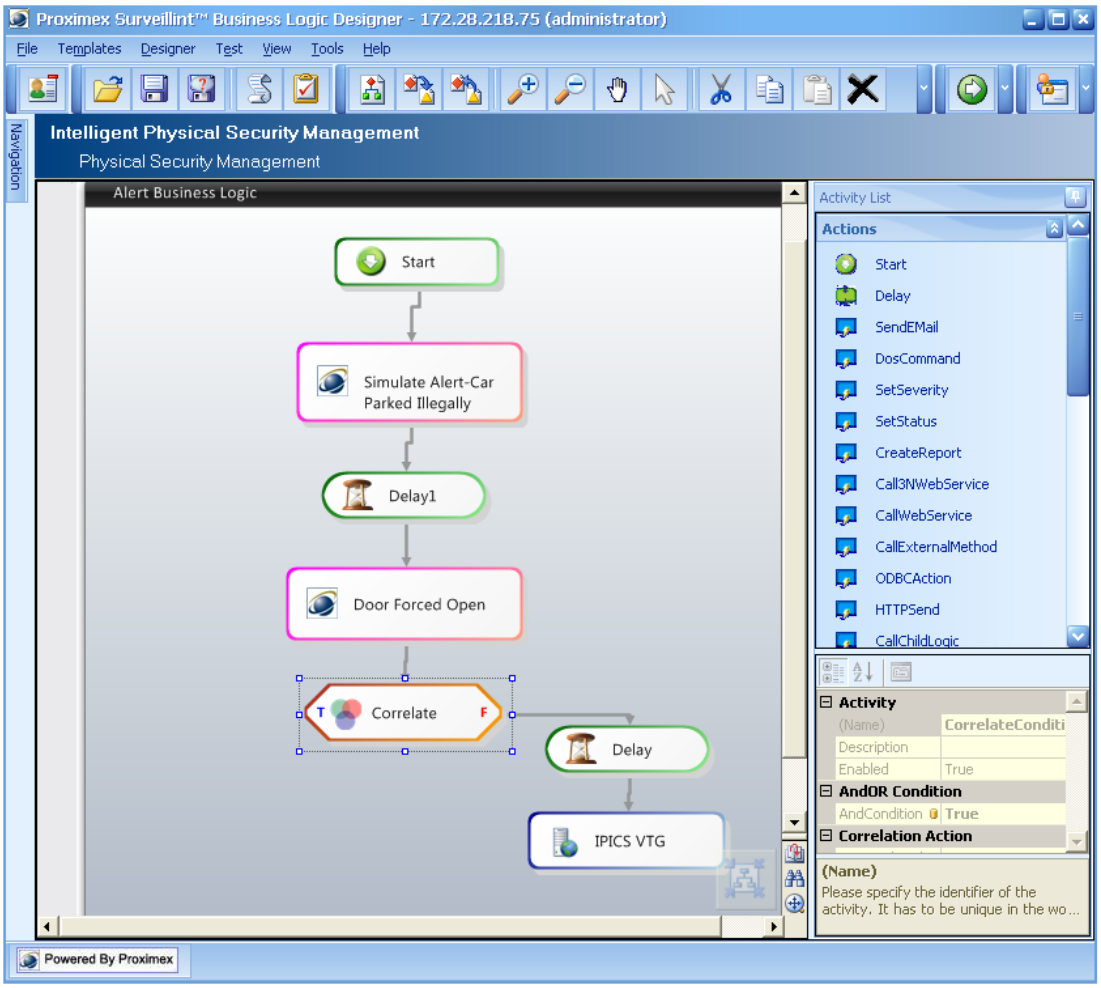
Surveillint's correlated alerts feature allow multiple alerts to be correlated across multiple systems to raise additional alerts, raise the severity of alerts, close or acknowledge existing alerts.

Correlated alerts allow alerts of a certain type across all sensors in an area to be grouped. When the area has multiple sensors (doors, cameras, and so on) and alerts on the sensors trigger within a short span of time, it's useful to gather these alerts together for further analysis.

Alerts can be correlated by time range, proximity by monitoring area or sensor group, severity level, alert description, or alert type. When the correlation criteria are met, the CorrelatedCondition icon in Business Logic can generate a new alert and update the status for severity of the existing correlated alerts.

The Business Logic in Figure 6-10 is used to correlate two alerts and to initiate a Virtual Talk Group with IPICS.

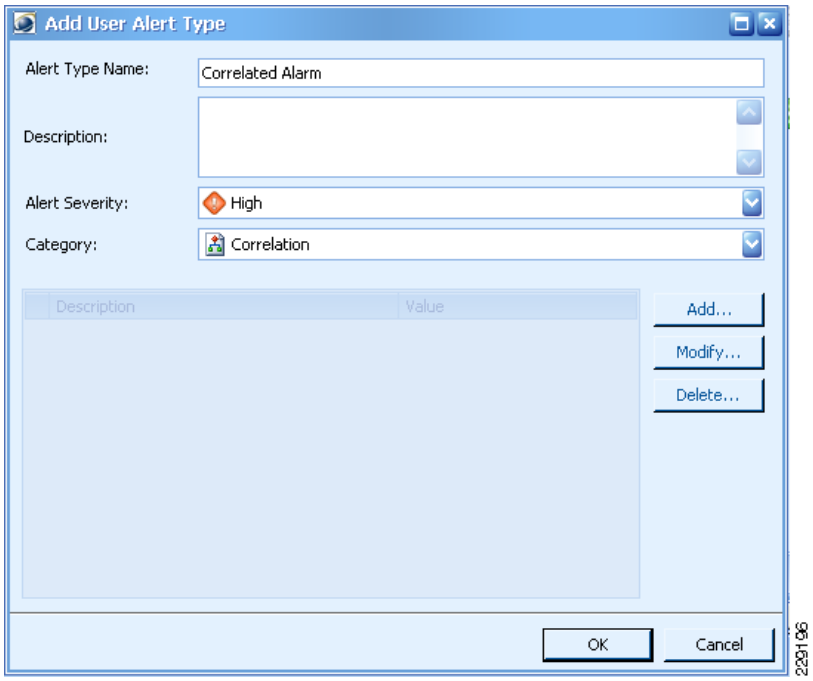
Figure 6-10 Correlated Alert



The first simulated alert is triggered by ObjectVideo after detecting a car parked illegally for more than 30 seconds. The second alert comes from Cisco Physical Access Manager and was triggered by a suspect forcing the door open.

To create the Correlated Alert under the Administration Console, select **Event Integration > User Alert Type > Add**. Define the proper alert severity and set the category to **Correlation**, as shown in Figure 6-11.

Figure 6-11 User Alert Type



From the Business Logic designer, the Correlate activity can be configured to match alerts created within 60 seconds matching two alert types: Door Forced Open and OnBoardUniversal (ObjectVideo). The severity of the correlated alert can also be set to Critical, because the incident has detected a car parked illegally and later on a door forced open. All these parameters can be easily selected and configured through the predefined correlate activity.

To define the two alerts being correlated, from the correlate activity, click the **Alert Type(s) matching** menu and select the relevant alert types.

Under **Alert Type**, select the alert defined in the previous step, ForcedDoor and Analytics.

Because the two events happened in the same area and took place within a certain time, the security operator is able to work on a single event, making the workflow operations and documentation more efficient.

Figure 6-12 shows the results of a correlated alert presented to the security operator, including both alerts: Door Forced Open from CPAM and Car Parked Illegally from ObjectVideo. The operator is also presented with the Response Workflow, or the SOP that should be followed to resolve the alert.

Figure 6-12 Alerts and Response Workflow

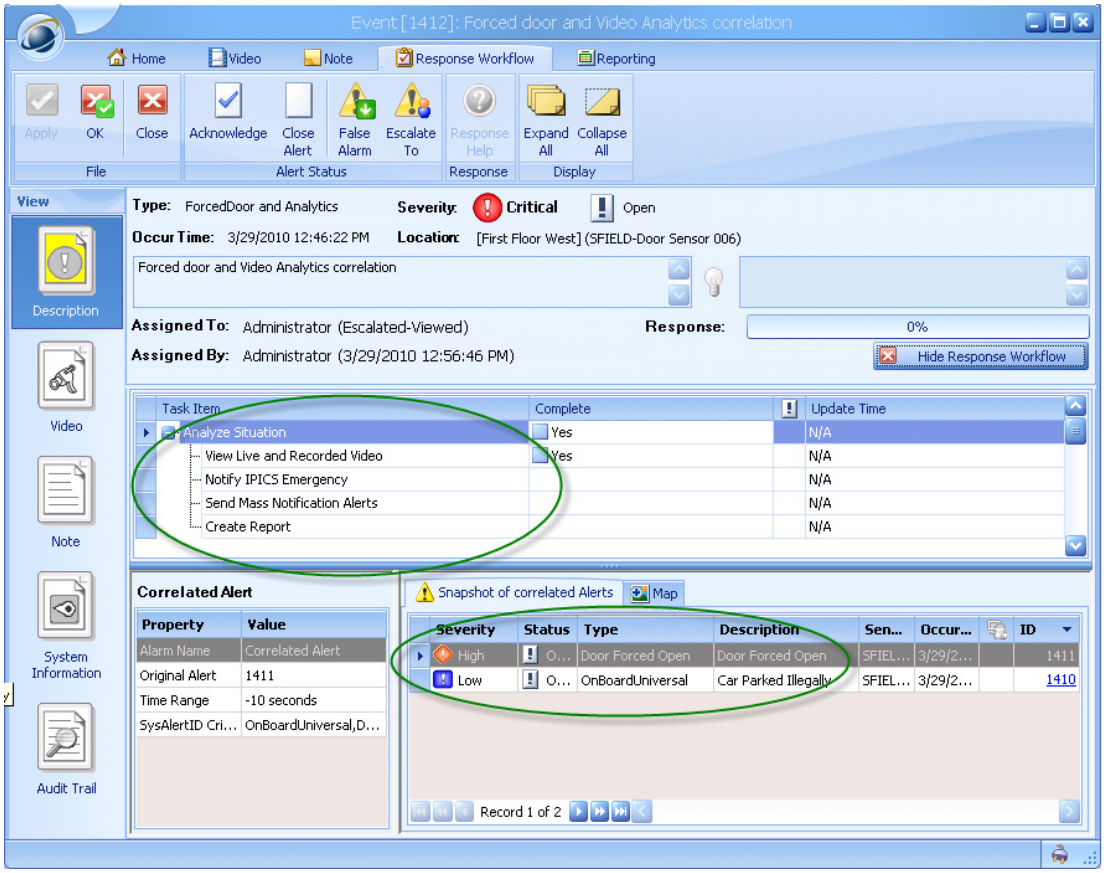
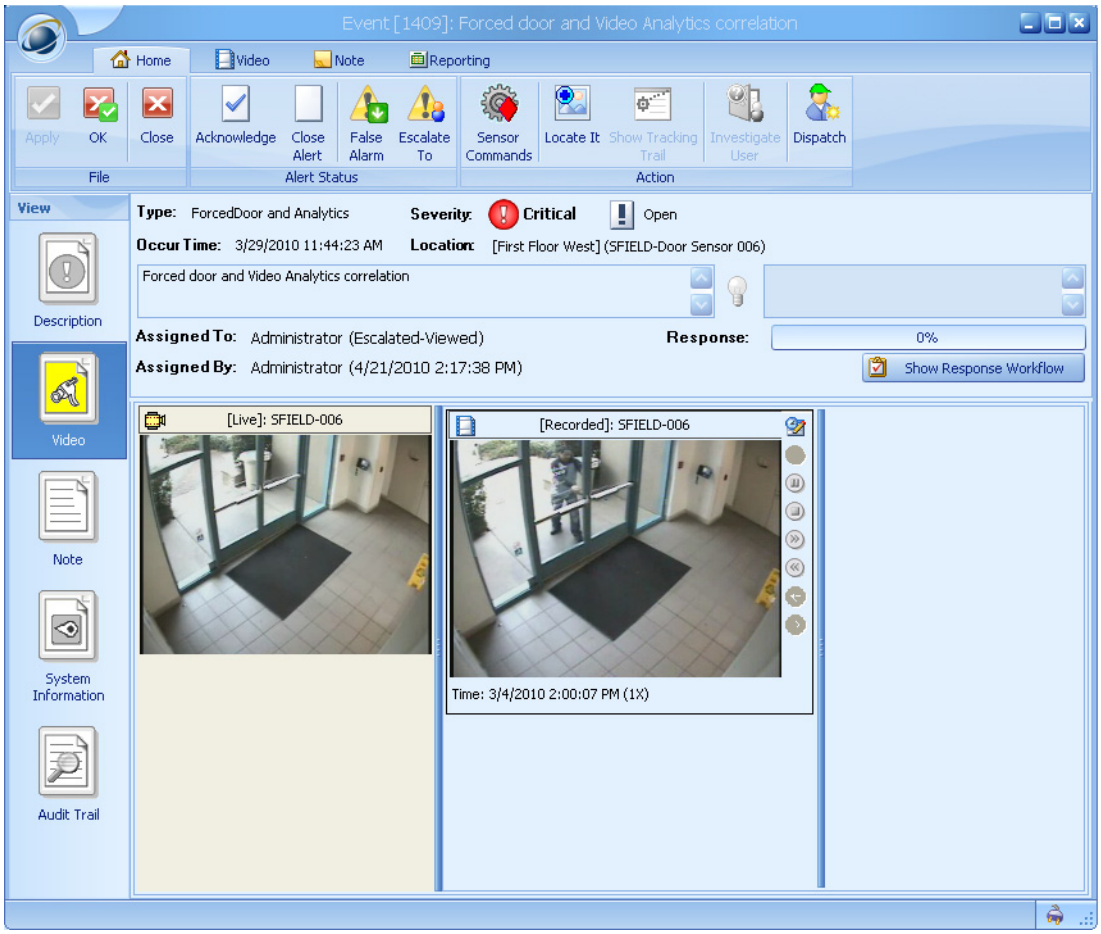


Figure 6-13 shows how the security operator is able to review live and recorded video from the same event window, reducing the number of errors and improving the time to resolve an incident.

Figure 6-13 Live and Recorded Video



From the same event window, the security operator is also able to perform other tasks, such as acknowledging or closing the alert, escalate it to another operator, locate it in a map, write notes, and so on.